CERT

Garbage Collection: Using Flow to Understand Private Network Data Leakage

Sid Faber
sfaber@cert.org

© 2010 Carnegie Mellon University

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JAN 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Garbage Collection: Using Flow to Understand Private Network Data Leakage**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
FloCon 2011, in Salt Lake City, Utah, on January 10-13, 2011.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

© 2010 Carnegie Mellon University

NO WARRANTY

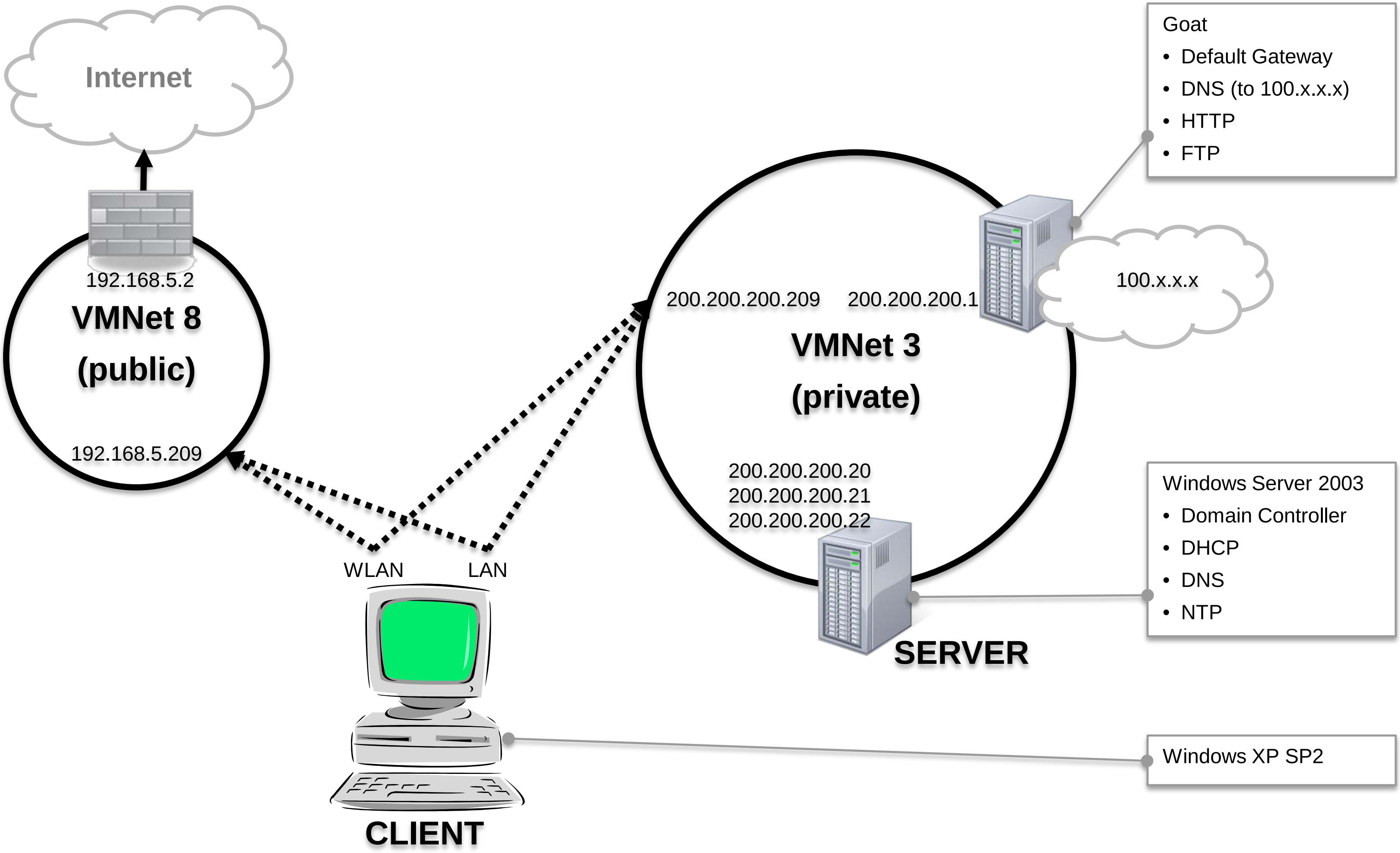
THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

CERT ® is a registered mark owned by Carnegie Mellon University.

Virtual Layout



Goat

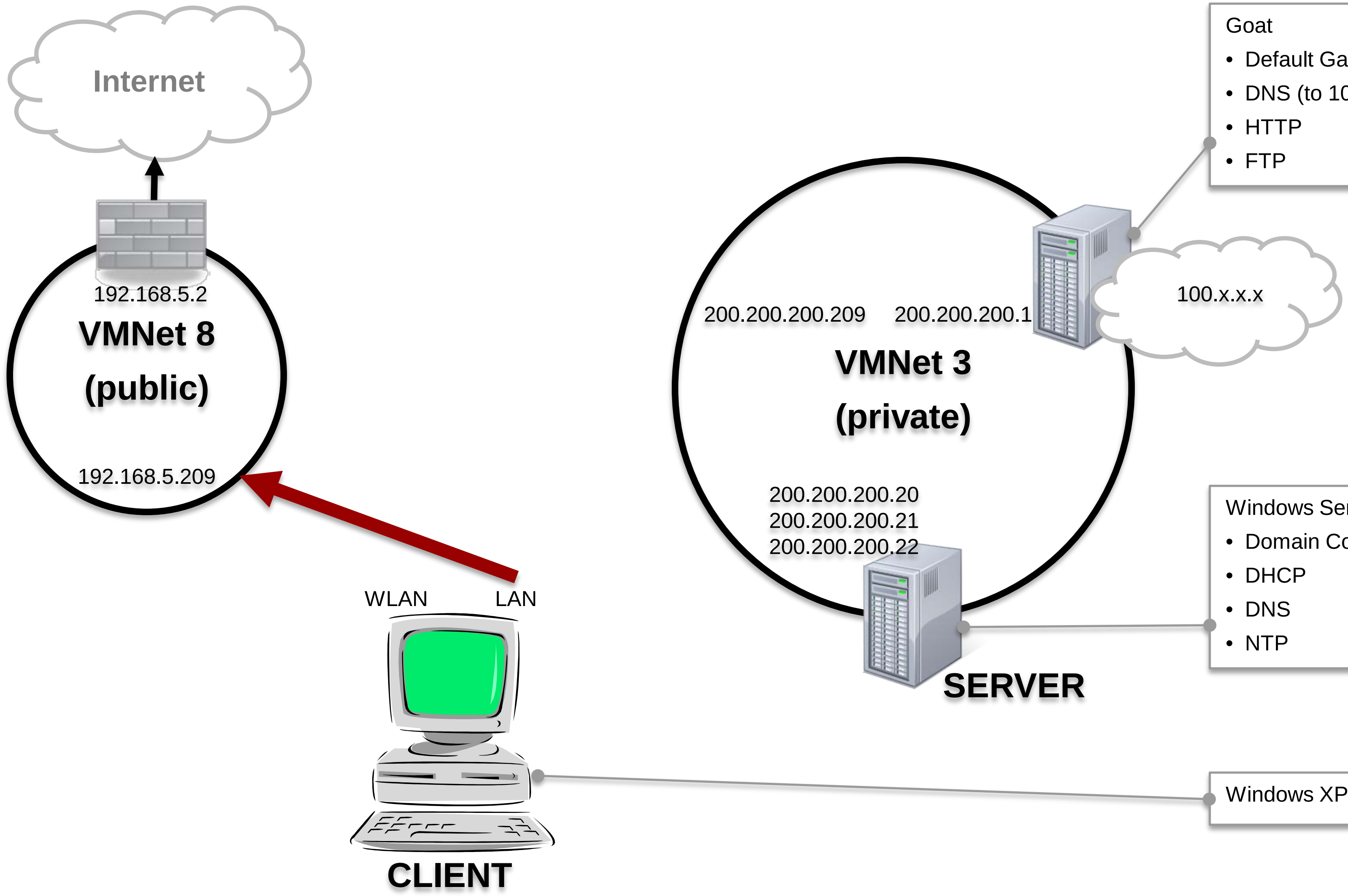
- Default Gateway
- DNS (to 100.x.x.x)
- HTTP
- FTP

Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Windows XP SP2

Experiment 1: Stand-alone boot



Goat

- Default Gateway
- DNS (to 100.x.x.x)
- HTTP
- FTP

Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Windows XP SP2

Experiment 1: Procedure

1. Start ethereal on HOST
2. Start ethereal on GOAT
3. Connect LAN on CLIENT to vmnet8
4. Start CLIENT
5. Verify internet connectivity: browse to www.cnn.com and get a legitimate web page
6. Stop packet capture on HOST and save as vmnet3.pcap.
7. Stop packet capture on GOAT and save as vmnet8.pcap.

Results 1: Stand-alone boot

```
|---------|-------------------|-------------------|-------------------|-------------------|
|Time     | 0.0.0.0           | 255.255.255.255   | 192.168.5.249     | 192.168.5.207     |
|---------|-------------------|-------------------|-------------------|-------------------|
|0.000    |         DHCP Request                  |                   |                   |
|         |(68)     ------------------>  (67)     |                   |                   |
|0.000    |                   |                   |         DHCP ACK      - Tra           |
|         |                   |                   |(67)     ------------------>  (68)     |
|---------|-------------------|-------------------|-------------------|-------------------|

|---------|-------------------|-------------------|-------------------|-------------------|-------------------|
|Time     | 192.168.5.207     | 192.168.5.2       | 192.168.5.255     | 224.0.0.22        | 207.46.232.182    |
|---------|-------------------|-------------------|-------------------|-------------------|-------------------|
|2.746    |         NBNS      |                   |                   |                   |                   |NBNS: Multi-homed registration NB CLIENT<00>
|         |(137)    ------------------>  (137)    |                   |                   |                   |
|7.296    |         NBNS      |                   |                   |                   |                   |NBNS: Registration NB CLIENT<00>
|         |(137)    -------------------------------------->  (137)    |                   |                   |
|10.312   |         NBNS      |                   |                   |                   |                   |NBNS: Registration NB WORKGROUP<00>
|         |(137)    ------------------>  (137)    |                   |                   |                   |
|14.835   |         NBNS      |                   |                   |                   |                   |NBNS: Registration NB WORKGROUP<00>
|         |(137)    -------------------------------------->  (137)    |                   |                   |
|18.358   |         NBNS      |                   |                   |                   |                   |NBNS: Multi-homed registration NB CLIENT<20>
|         |(137)    ------------------>  (137)    |                   |                   |                   |
|25.888   |         NBNS      |                   |                   |                   |                   |BROWSER: Host Announcement CLIENT, Workstation, Serv
|         |(138)    -------------------------------------->  (138)    |                   |                   |
|26.726   |         DNS       |                   |                   |                   |                   |DNS: Standard query A time.windows.com
|         |(1025)   ------------------>  (53)     |                   |                   |                   |
|27.900   |         IGMP      |                   |                   |                   |                   |IGMP: V3 Membership Report / Join group 239.255.255.
|         |(0)      ---------------------------------------------------------->  (0)      |                   |
|---------|-------------------|-------------------|-------------------|-------------------|-------------------|
```

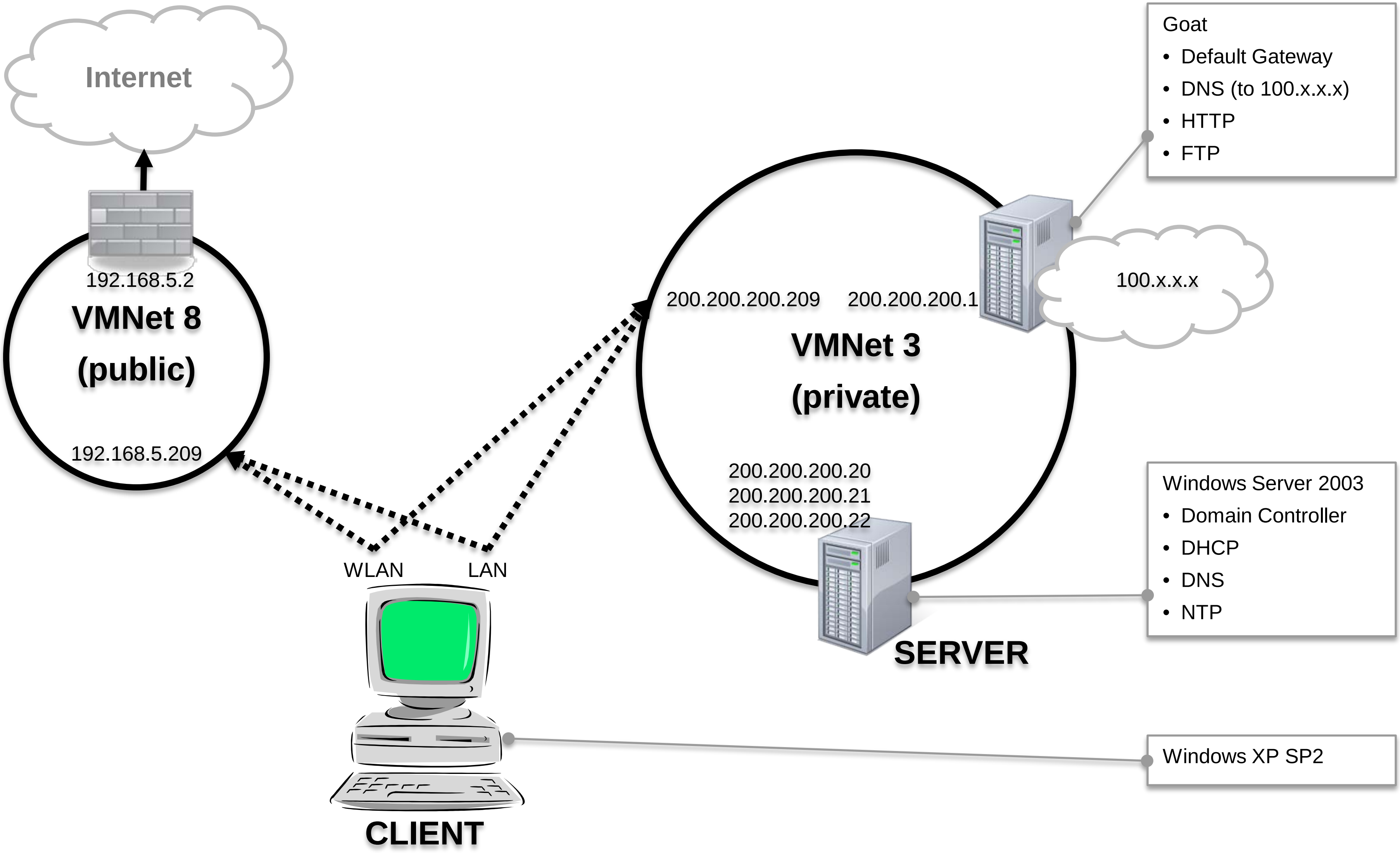
[continued]

Results 1: Stand-alone boot (2)

```
|---------|-------------------|-------------------|-------------------|
|Time     | 192.168.5.207     | 192.168.5.2       | 207.46.232.182    |
|---------|-------------------|-------------------|-------------------|
|28.807   |         DNS       |                   |                   |DNS: Standard query A time.windows.com
|         |(1025)   ------------------>  (53)     |                   |
|30.749   |         DNS       |                   |                   |DNS: Standard query response CNAME time.microsoft.akadns.net A 207.46.232.182
|         |(1025)   <------------------  (53)     |                   |
|30.822   |         NTP       |                   |                   |NTP: NTP symmetric active
|         |(123)    -------------------------------------->  (123)    |
|---------|-------------------|-------------------|-------------------|


|---------|-------------------|-------------------|-------------------|
|Time     | 192.168.5.207     | 192.168.5.2       | 157.166.226.25    |
|---------|-------------------|-------------------|-------------------|
|72.489   |         Standard query A ww           |                   |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)     |                   |
|73.490   |         Standard query A ww           |                   |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)     |                   |
|74.491   |         Standard query A ww           |                   |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)     |                   |
|76.492   |         Standard query A ww           |                   |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)     |                   |
|76.604   |         Standard query resp           |                   |DNS: Standard query response A 157.166.226.25 A 157.166.226.26 A 157.166.255.18 A 157.166.25
|         |(1025)   <------------------  (53)     |                   |
|76.625   |         iad3 > http [SYN] S           |                   |TCP: iad3 > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
|         |(1032)   -------------------------------------->  (80)     |
|76.670   |         http > iad3 [SYN, A           |                   |TCP: http > iad3 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
|         |(1032)   <--------------------------------------  (80)     |
|76.682   |         iad3 > http [ACK] S           |                   |TCP: iad3 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
|         |(1032)   -------------------------------------->  (80)     |
|76.722   |         GET / HTTP/1.1                |                   |HTTP: GET / HTTP/1.1
|         |(1032)   -------------------------------------->  (80)     |
|76.722   |         http > iad3 [ACK] S           |                   |TCP: http > iad3 [ACK] Seq=1 Ack=455 Win=64240 Len=0
|         |(1032)   <--------------------------------------  (80)     |
|---------|-------------------|-------------------|-------------------|
```

Scenario 2: Standalone boot on private



Internet

192.168.5.2

VMNet 8

(public)

192.168.5.209

200.200.200.209

200.200.200.1

VMNet 3

(private)

200.200.200.20
200.200.200.21
200.200.200.22

100.x.x.x

WLAN

LAN

CLIENT

SERVER

Goat

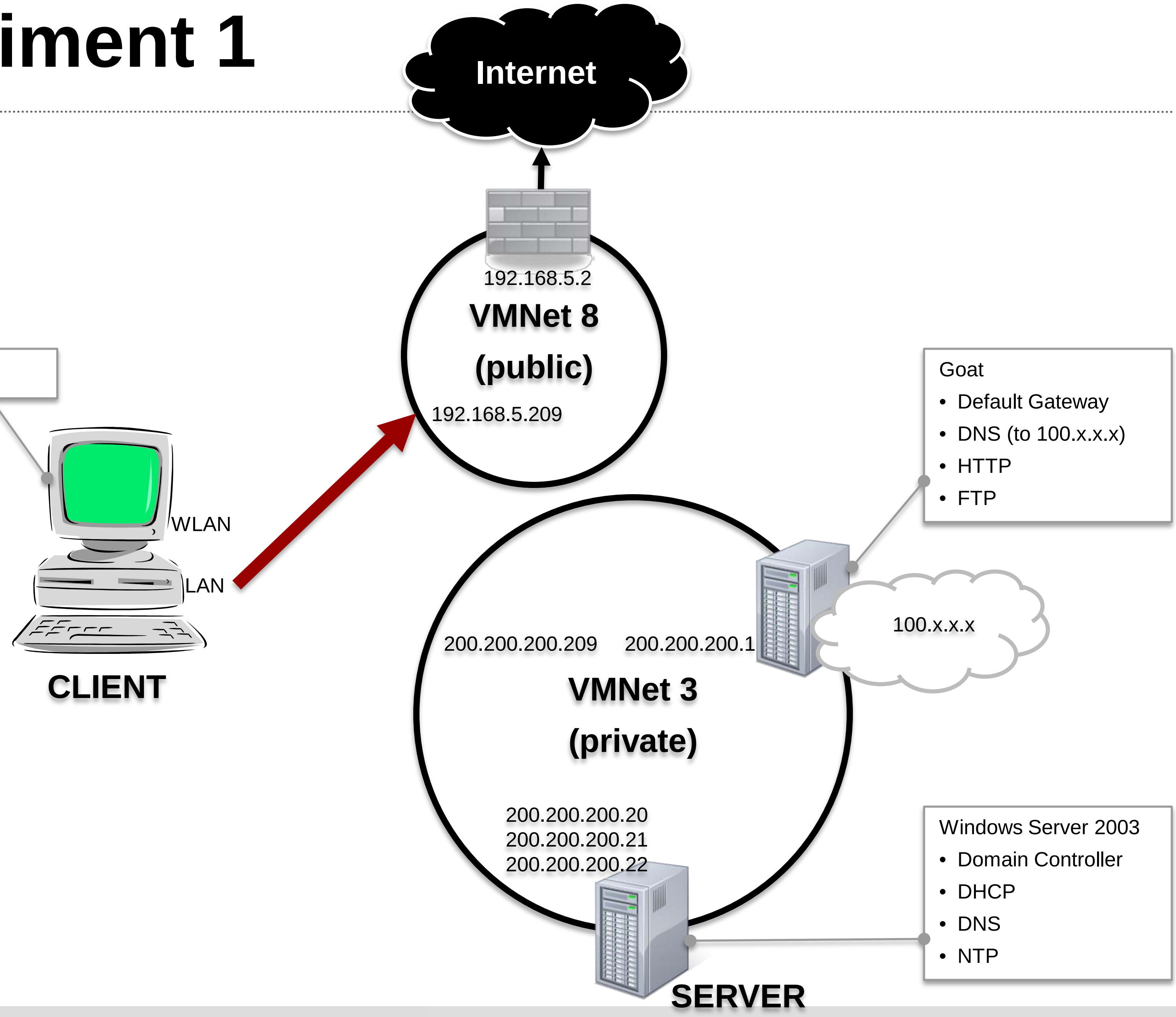
- Default Gateway
- DNS (to 100.x.x.x)
- HTTP
- FTP

Windows Server 2003

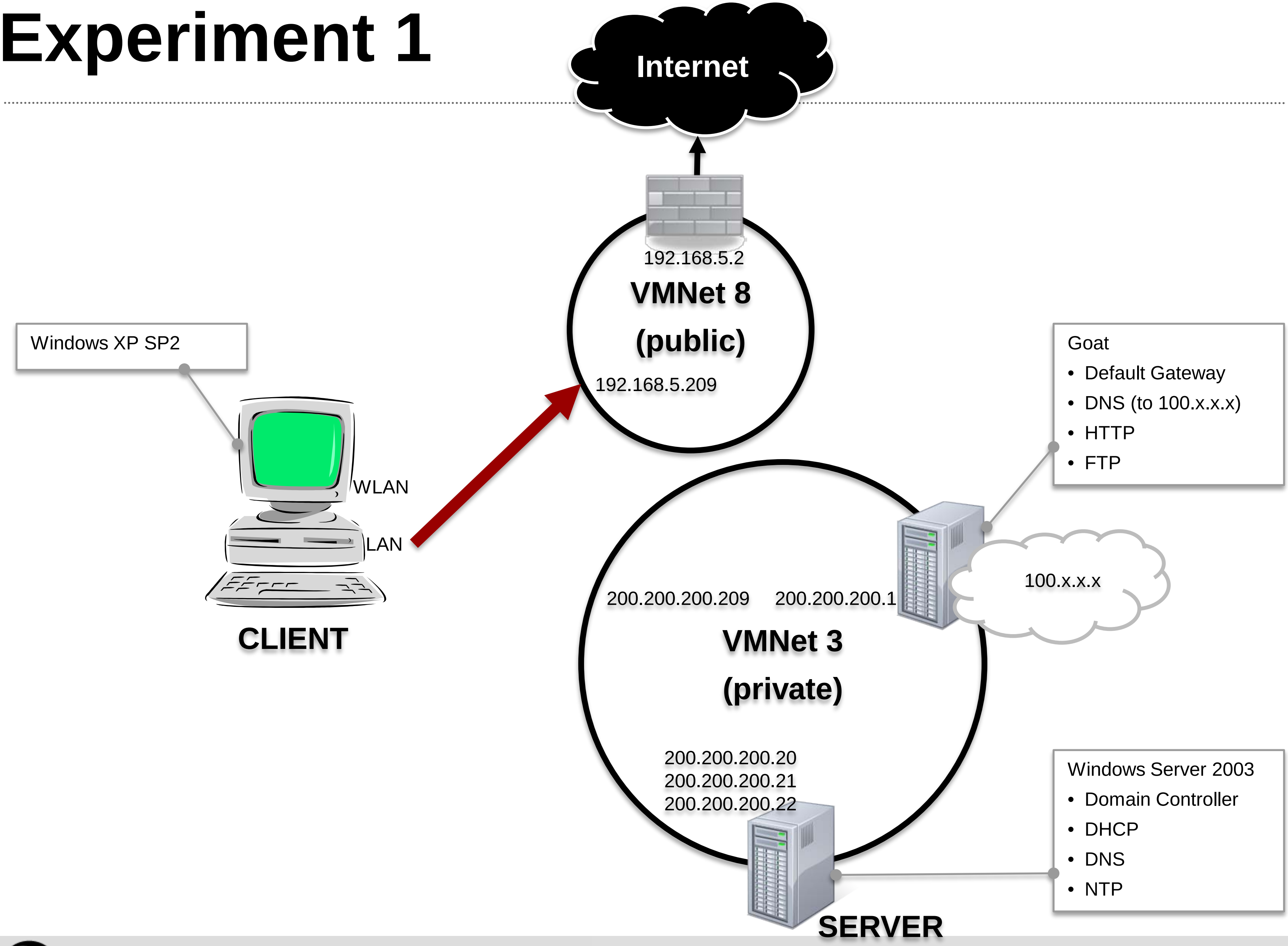
- Domain Controller
- DHCP
- DNS
- NTP

Windows XP SP2

Experiment 1



Experiment 1



Windows XP SP2

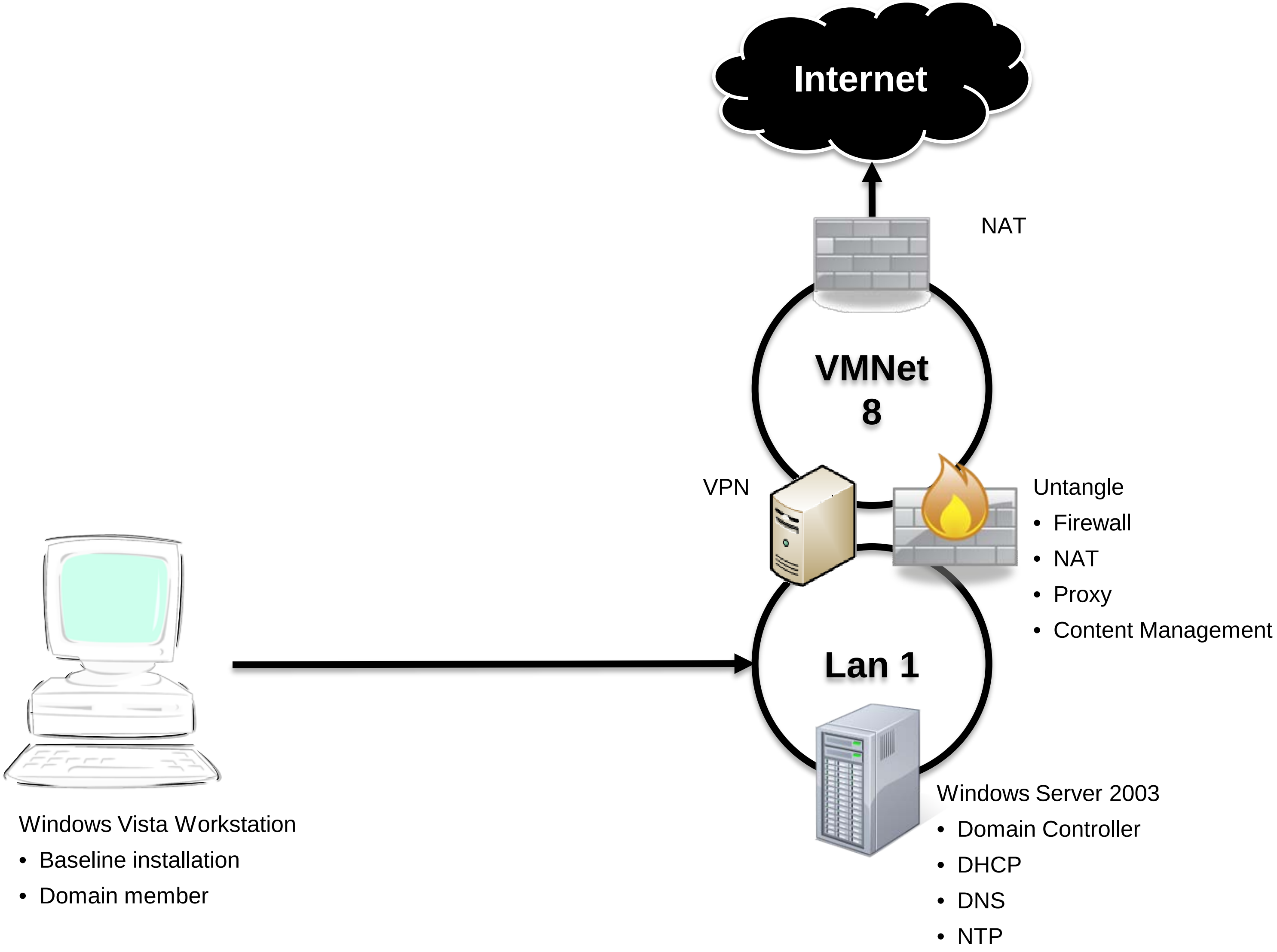
Goat

- Default Gateway
- DNS (to 100.x.x.x)
- HTTP
- FTP

Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Scenario 1: Restart on Another Network



Untangle

- Firewall
- NAT
- Proxy
- Content Management

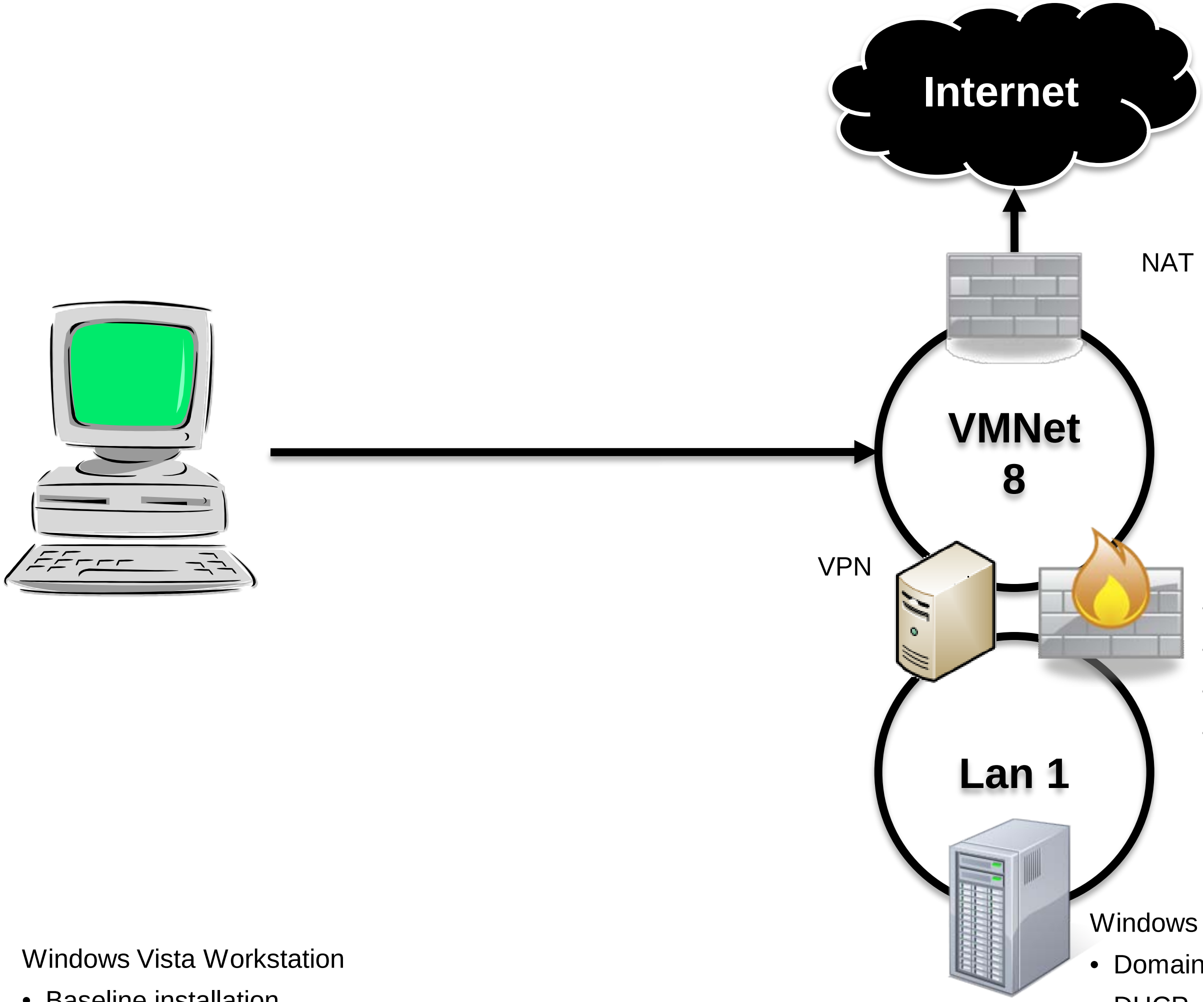
Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Windows Vista Workstation

- Baseline installation
- Domain member

Scenario 1: Restart on Another Network



Untangle

- Firewall
- NAT
- Proxy
- Content Management

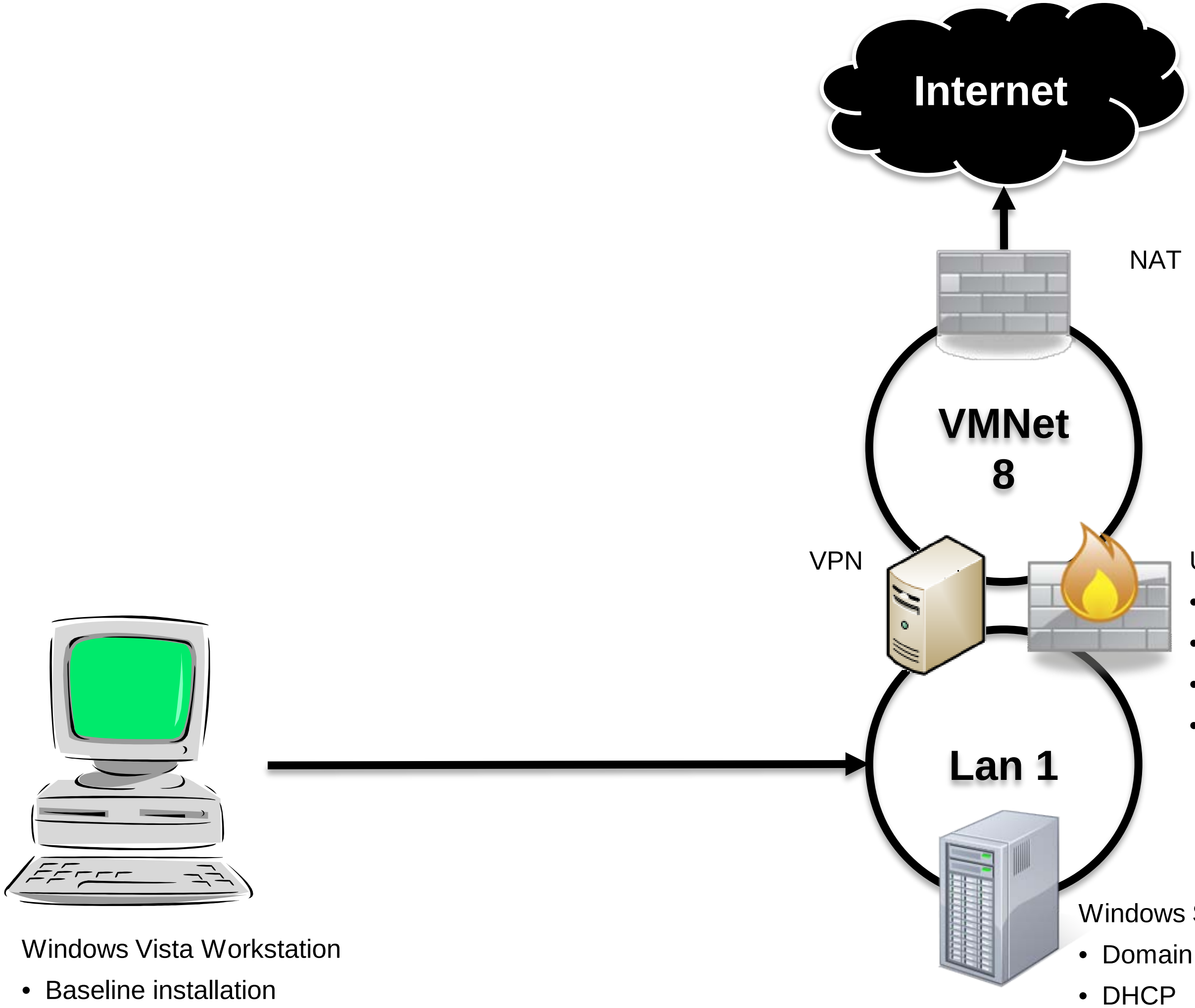
Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Windows Vista Workstation

- Baseline installation
- Domain member

Scenario 2: Move to Another Network



Untangle

- Firewall
- NAT
- Proxy
- Content Management

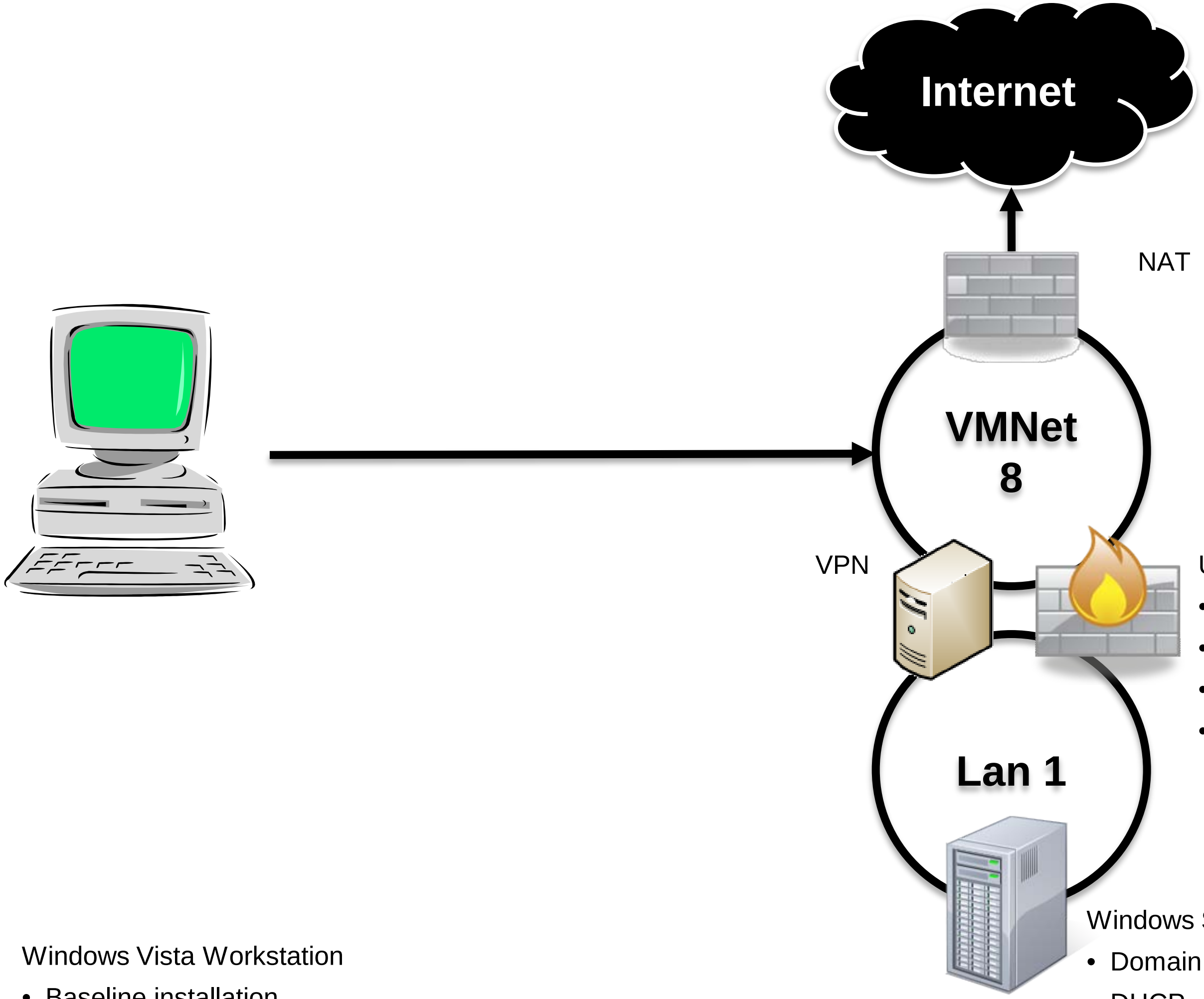
Windows Vista Workstation

- Baseline installation
- Domain member

Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Scenario 2: Move to Another Network



Untangle

- Firewall
- NAT
- Proxy
- Content Management

Windows Server 2003

- Domain Controller
- DHCP
- DNS
- NTP

Windows Vista Workstation

- Baseline installation
- Domain member